Michigan State Police
Emergency Management & Homeland Security

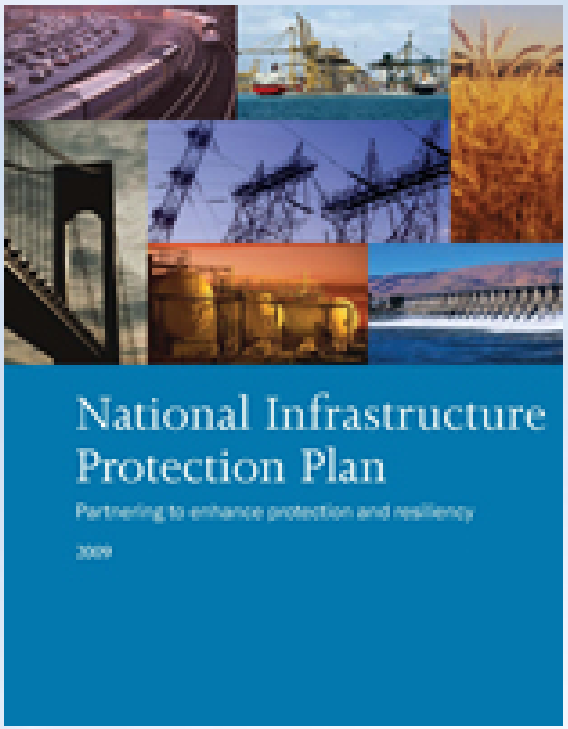
Infrastructure Analysis & Response Section

Sgt. Bruce E. Payne

Presidential Directive

On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7) which establishes a National policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

National Infrastructure Protection Plan



As a result of Homeland Security Presidential Directive 7 (HSPD-7) 18 sectors were identified at the National level for the National Infrastructure Protection Plan (NIPP).

Agriculture & Food Sector

Prevent the contamination of the food supply that would pose a serious threat to public health, safety and welfare.

Banking & Finance

The banking and Finance Sector accounts for more then eight percent of the U.S. annual gross domestic product and is the backbone for the world economy.

Chemical Sector

The Chemical Sector is comprised of several hundred thousand facilities in the United State that can be characterized in three main functional areas:
Manufacturing plants, transport systems, and distribution systems.

Commercial Facilities

- This sector includes a wide range of businesses, commercial, residential, and recreational facilities where large numbers of people congregate.

- This sector operates on the principle of "open public access".

- Primarily exists of "soft targets"

Communications

The Communications Sector is characterized as a diverse, open, highly competitive, and interconnected industry, which includes technologies and services such as wire line, wireless, satellite, cable, broadcast, Internet, and other key information systems.

Critical Manufacturing

The Critical Manufacturing Sector is crucial to the economic prosperity and continuity of the United States. U.S. manufacturers design, produce, and distribute products that provide more than one of every eight dollars of the U.S. gross domestic product and employ more than 10 percent of the nation's workforce.

Dams Sector

The Dams Sector is a vital component of the Nation's critical infrastructure and key resources. These assets enable water management and supply, hydroelectric power generation, navigable waterways, irrigation, flood damage control, storm surge protection, recreation, wildlife habitat sustainability, and environmental stability.

Defense Industrial Base

The Defense Industrial Base includes hundreds of thousands of worldwide industrial facilities with varying capabilities to perform research and development, design, produce, deliver, and maintain military weapons systems.

Emergency Services

The Emergency Services Sector is a system of preparedness, response, and recovery elements that forms the Nation's first line of defense for preventing and mitigating the risk from terrorist attacks and manmade and natural disasters.

Energy Sector

The Energy Sector consists of thousands of electricity, oil, and natural gas assets that are geographically dispersed and connected by systems and networks.

Government Facilities

The Government Facilities Sector includes facilities owned or leased by all levels of government for the purpose of conducting official government business. This sector is to establish a preparedness posture that ensures the safety and security of government facilities so that essential government functions and services are preserved without disruption.

Information Technology

The Information Technology Sector enables more than $3 trillion worth of economic activity to pass through secure Federal financial networks on a daily basis. Critical Infrastructure and key resource sectors rely on the Information Technology for products and services, including the reliable operations of network and systems and the movement and storage of critical data.

National Monuments & Icons

The National Monuments and Icons Sector is committed to ensuring that the symbols of our Nation remain protected and intact for future generations. In the course of protecting our landmarks, the sector will ensure that staff and visitors are protected for harm.

Nuclear Sector

The Nuclear Sector provides power to millions of homes and businesses across the country.

3 Nuclear Power Plants in Michigan

- **D.C. Cook Nuclear Plant**
- **Fermi Power Plant**
- **Palisades Power Plant**

Postal and Shipping

The Postal and Shipping Sector contains multi-layered networks of collection, transportation, and distribution assets. This sector's continuity of business plans envisions a resilient infrastructure in which threats can be quickly detected, consequences localized, and operational disruptions minimized.

Public Health & Healthcare

Ensuring a resilient healthcare system capable of withstanding disruption and poised to provide emergency services for the Nation's safety and security.

Transportation Systems

The Transportation Systems Sector includes all modes of transportation that move millions of passengers and goods in a vast interdependent network.

Water Sector

The United States has one of the safest water systems in the world. Since water is essential for life and the operation of many other sectors, the Water Sector has developed multi-layered physical, cyber, and human security protective programs.

Education Sector

Michigan was the first state to identify education as a critical infrastructure. With the addition of education, Michigan has a total of 19 sectors.

Sector-Specific Plans

- Contained within the NIPP each sector has a supporting Sector-Specific Plans (SSPs) that provides a coordinated approach that will be used to establish national priorities, goals, and requirements for critical infrastructure and key resources (CI/KR) protection.

- Contained within each (SSPs) is the overview, vision, goals, priorities, challenges, and interdependencies for the 18 Nationally recognized sectors. The (SSP) for the Education Sector will be contained with the (MIPP).

MIPP (Michigan Infrastructure Protection Plan)

The MIPP presents a road map for the implementation of Michigan's Critical Infrastructure and Key Resources (CIKR) program. The plan is comprised of the following sections:

- Organizational Roles and Responsibilities will detail the State of Michigan's Homeland Security roles and responsibilities of state agencies, committees, and other organizations created for CIKR protection.
- Critical Infrastructure Protection Laws and Regulations will detail laws and regulations currently in place for protecting Michigan's Infrastructure as well as critical infrastructure information.
- Critical Infrastructure Protection Capabilities and Assets will detail assets available and utilized by the states homeland security for protecting infrastructure.
- Critical Infrastructure Protection Accomplishments will provide key activities accomplishments which achieve previously set goals and plans to provide additional critical infrastructure protection.
- Critical Infrastructure Protection Goals and Plans will outline future goals and plans the State of Michigan desires to accomplish for enhanced infrastructure protection.

Infrastructure Analysis & Response Section

- Primary & Secondary Agents for all sectors
- ACAMS monitoring for CI/KR for Michigan
- Site Assessment Visits (SAV) for CI/KR Sites
- Protected Critical Infrastructure Information (PCII)
- Development of the MIPP
- Assist with the development of Safety Plans
- Assist with drills and training employees/ students
- Response/Assist Team- provide AAR
- Facilitate (DHS) Special Events data call.
- Facilitate (DHS) Tier 1 and Tier 2 data call for critical infrastructure.
- MICC (Michigan Infrastructure Coordinating Committee) - Member identification, roles, alliance and coordination to create a network between the private and public sectors.

ACAMS

Automated Critical Asset Management System (ACAMS) is a secure, Web-based information services portal used to support infrastructure protection efforts at the state and local level. It provides access to a comprehensive set of tools and resources to develop and implement CIP (Critical Infrastructure Protection) programs.

While ACAMS focuses on pre-incident prevention and protection it also assists in post-incident response. ACAMS leverages the close relationship between local law enforcement, first responders and asset owner/operators. CIKR owners/operators are a key partner in planning and use of ACAMS and its success depends on Public/Private Partnerships. State and local personnel interact daily with CIKR (Critical Infrastructure Key Resources) owners and operators to maintain detailed, accurate infrastructure data.

Benefits of ACAMS

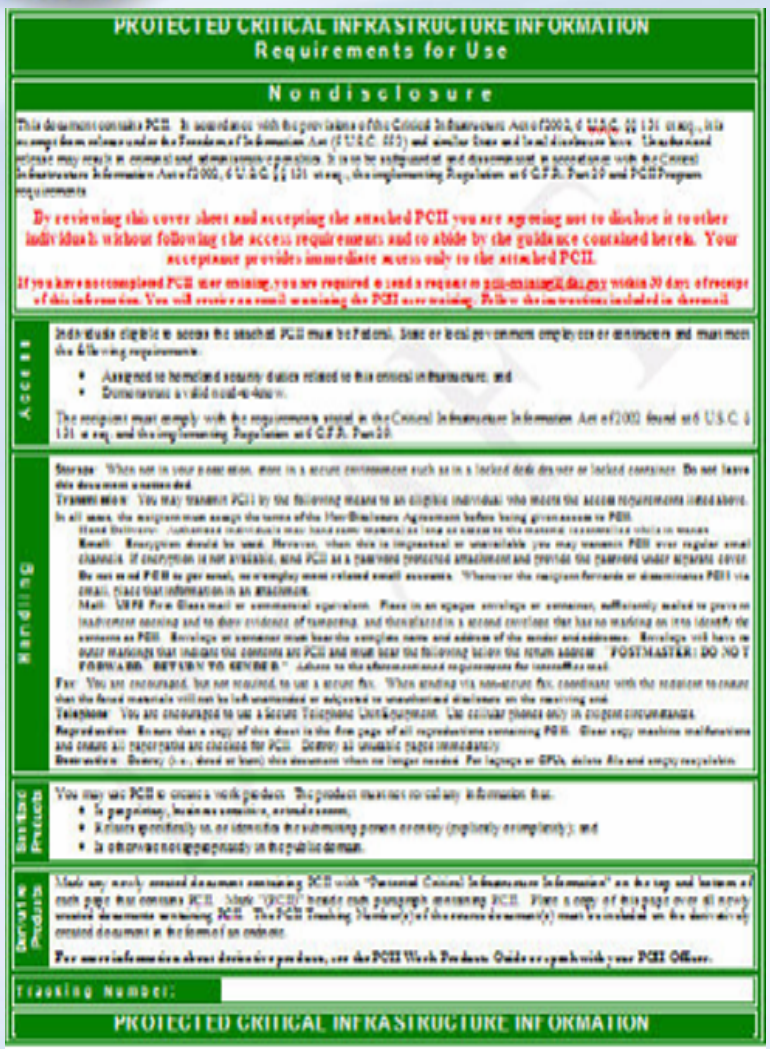
ACAMS provides a set of tools and resources to help law enforcement, public safety and emergency response personnel by:

- Collecting and using CIKR asset data
- Assess CIKR asset vulnerabilities
- Develop all-hazards incident response and recovery plans
- Enables First responders to know the assets response plans
- Provides for the input of assets floor plans/diagrams/images
- Takes the guess work out of responding to an incident
- Build public-private partnerships
- Saves lives

ACAMS USERS

- State and local emergency responders
- Infrastructure protection planners
- Homeland security officials
- Public safety (police & fire)
- Emergency managers

Protected Critical Infrastructure Information (PCII)



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

This document contains PCII. In accordance with the provisions of the Critical Infrastructure Act of 2002, 6 U.S.C. §§ 131 et seq., it is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq., the implementing Regulation at 6 C.F.R. Part 29 and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the Critical Infrastructure Information Act of 2002 (found at 6 U.S.C. § 131 et seq. and the implementing Regulation at 6 C.F.R. Part 29).

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. Do not leave this document unattended.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of a Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. Do not send PCII to personal, non-employer owned email accounts. Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "POSTMASTER: DO NOT FORWARD. RETURN TO SENDER." Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via unsecured fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Derivative Products

You may use PCII to create a work product. The product must not contain any information that:

- Is proprietary, business sensitive, or trade secret;
- Is classified national security information (unless appropriately marked and protected); and
- Is otherwise appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Tracking Number(s) of the source document(s) must be included on the derivative document in the form of an endnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Tracking Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

- Enables members of the private sector to voluntarily submit sensitive information regarding the nation's critical infrastructure to the Department of Homeland Security (DHS) with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure.
- Protected Critical Infrastructure Information (PCII) and is not subjected to being accessed through the Freedom of Information Act, state and local disclosure laws and use in civil court.
- PCII protected information received via ACAMS is only disseminated to first responders in the time of need and is not to be disseminated to any unauthorized individual

SAV Team

- The Critical Asset Assessment Team (CAAT) initiative, housed within the Michigan State Police, Emergency Management and Homeland Security Division, Infrastructure Analysis and Response Section, assists the owner/operator of Critical Infrastructure/Key Resources in Michigan in identifying site vulnerabilities and understanding and developing mitigation strategies.

- The assessment tool utilized by the CAAT teams was developed by DHS and is known as the SAV (Site Assistance Visit).

- The SAV process brings together owners and operators with other security partners in developing joint mitigation strategies and facilitates the sharing of information.

- The SAV process is flexible and applicable across all 18 identified CI/KR sectors.

SAV Definition

- The SAV is designed to facilitate vulnerability identification and mitigation discussions between the CAAT members and the site owner/operator.
- The SAV is an information gathering visit. The visit is non-regulatory and is not an inspection and there is no pass-fail grade given. At the end of the SAV, an out briefing will be conducted and a completed report will be given to the asset owner.
- All hazards approach assessment
- The asset population into ACAMS can also be a part of the SAV visit.

SAV Purpose

- Develop an awareness of a site's physical vulnerability to terrorist attack and systems connectivity, interdependency and weaknesses.

- Create a site-specific report from visit observations, expert inputs and background data;

  - Confidential information is used to enhance the security

  - Information is protected under the Protected Critical Infrastructure Information (PCII) program.

MICC

- The Michigan Infrastructure Coordinating Committee (MICC) was formed in March 2008 under the guidance of the Michigan State Police, Emergency Management and Homeland Security Division—Infrastructure Analysis and Response Section (IARS) after the need for private/public partnership was identified. The MICC is chaired by the IARS Commander and is co-chaired by a private sector member. The MICC was created to bring together members of public and private industry to address preparedness issues related to protecting critical infrastructures and key resources.

MICC Purpose

MICC is to support the goals and objectives of the (NIPP) and the (MIPP) to strengthen the partnership between the public and private sector.

Areas of concern include:

- Alert Notification
- Threat Response
- Prioritization Efforts
- Special Events Planning
- Information Sharing Mechanisms
- NIPP Implementation & Compliance
- Threat & Vulnerability Assessments of CIKR
- Department of Homeland Security Annual Data Call for prioritizing Critical Infrastructure sites within the State of Michigan

Bringing it all together

DVD Presentation

“2009 National Infrastructure Protection Plan”

(NIPP in Action)

Prior Training

“7 Signs of Terrorism”

- DVD available
- Hand out
- Train with you employees

Questions

Contact information:

Sgt. Bruce Payne

Michigan State Police Emergency Management & Homeland Security

(517) 336-6655 (Office)

(517) 712-1332 (Mobile)

Payneb@michigan.gov